THE
POLESTAR
FOUNDATION

21st ANNUAL POLESTAR AWARDS
WINNERS DOSSIER

21st Annual PoleStar Awards

Celebrating Excellence in Journalism

The PoleStar Awards recognize outstanding talent among Indian media professionals and celebrate stupendous contributions from media citizens who have acted as catalysts in disseminating quality information to the world.

The PoleStar Foundation conceptualized the PoleStar Awards, way back in 1998 to mark excellence in IT and Business Journalism and since 2017 has added the celebration of Good News Feature as well!

BEST FEATURE IN TECHNOLOGY JOURNALISM

G Seetharaman and Rahul Sachitanand

G Seetharaman and Rahul Sachitanand won the Polestar Award for Best Feature in Technology Journalism for their article **'Breach Suspected',** which appeared in **The Economic Times on 22nd July, 2018.**

G Seetharaman and Rahul Sachitanand won the Polestar Award for Best Feature in Technology Journalism for their article 'Breach Suspected', which appeared in The Economic Times on 22nd July, 2018. Seetharaman, a Senior Assistant Editor in The Economic Times, is a Mumbai-based journalist with 11 years of experience. He began his career as a business journalist with Daily News and Analysis (DNA), followed by a brief stint at Business Today. He has been a feature writer with The Economic Times since 2013, covering a range of beats, including business, technology, energy, science and politics.

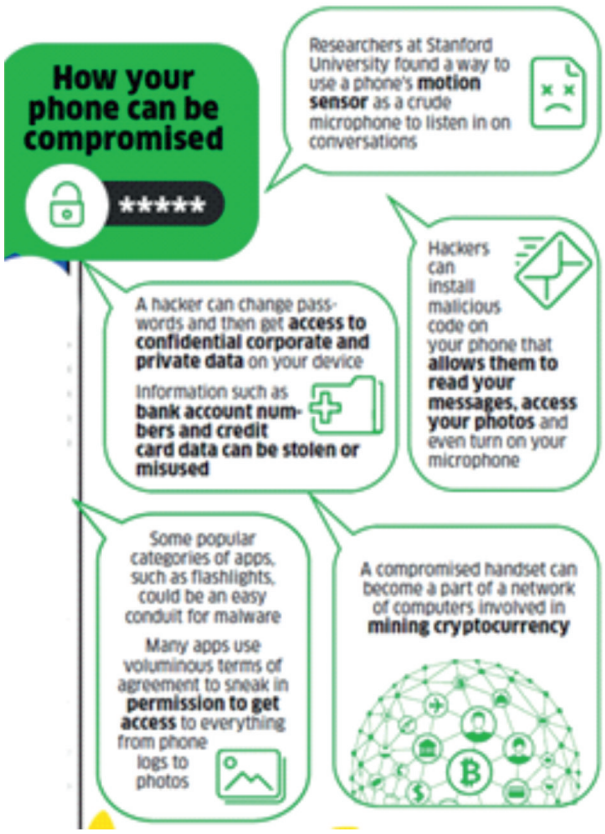
Rahul Sachitanand, who calls Bengaluru his home, is a freelancer with nearly two decades of experience in journalism, primarily in the long-form writing. He has worked with India's largest business publications and top editors of this time. Rahul has also worked in Mumbai and is currently based in Hong Kong as a freelance content creator. He is a graduate from the Asian College of Journalism, Chennai, with a specialisation in print journalism.

Breach Suspected!

Millions of first-time smartphone users, lack of data privacy regulation and devices running on outdated versions of Android together form a critical flaw at the heart of India's mobile security

G Seetharaman and Rahul Sachitanand

The Economic Times | 22nd July, 2018.



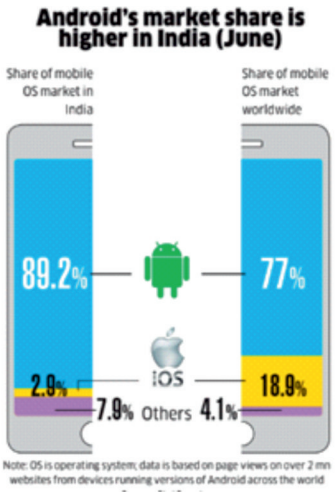
Saket Modi must have had possession of one of our phones — a Gionee M5 Lite running Android — for a little under a minute. All he did was make a few keystrokes, as far as we could tell. He didn't know its number nor did he attach a cable to it.

In a few seconds, much of the phone's data was sitting neatly on his computer. He now knew the list of calls that were made from the phone, the content of all text messages and details of their recipients, the list of contacts and the GPS coordinates that tell location — in this case, the Delhi-based offices of Lucideus, the cyber security firm run by Modi, a well-known ethical hacker.

What Modi did was install a piece of software code that can run in the background undetected by a user. A hacker can install it on a phone without having physical access to it. By sending a text or email couched as a promotional message that lures a user into clicking, for instance. A few minutes after he returned the phone to us, he demonstrated an even more unsettling trick. He played back snatches of our conversation, which he was able to surreptitiously record using the compromised phone's microphone. In other words, once hackers access your device, they can easily use your microphone or camera to record you, and thanks to GPS, they know your location. It's a security nightmare.

Companies that make operating systems (OS) for mobile phones — Apple's iOS and Google's Android occupy bulk of the market — know the array of techniques used by hackers to compromise phones. They are in a cat-and-mouse game with the rogue elements of the information age. They plug known vulnerabilities and loopholes by periodically updating their operating systems. They release newer versions of it and also issue security patches.

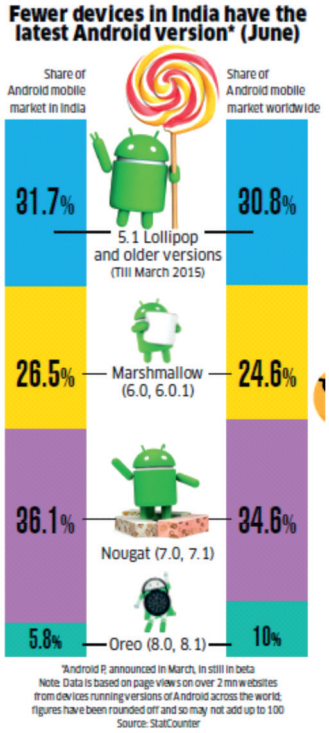
But in the case of Android, on which 9 out of 10 mobile phones in India run, there is a unique problem. Android is a foundational OS on which some of the most popular handset makers — such as Samsung or Xiaomi — build their versions of the operating system. This means when Android releases an update or a security patch, it's unclear who is responsible for updating the OS that's actually running on the device.



Phone makers release an update months after Android, if at all. There are hundreds of companies making Android-based devices, selling more than 60,000 models worldwide. It's a complex ecosystem, with no one quite tracking the updates and vulnerabilities.

A third of the Android phones in India are running a version of the OS released in March 2015 or before, according to analytics firm StatCounter. This leaves millions of phone users in India potentially vulnerable, and in an age when personal information harvested at scale can be weaponised to sway opinion and indeed elections, this hole at the heart of India's mobile security deserves wider attention. India has witnessed explosive growth in handset sales and data usage. There are now some 300 million smart phone users in India, the world's second biggest smartphone market after China.

This is expected to swell to just under 500 million by 2022, according to research firm eMarketer. With the entry of Reliance Jio, data costs have become affordable to just about anyone who can buy a smartphone. This means millions of excited first-time



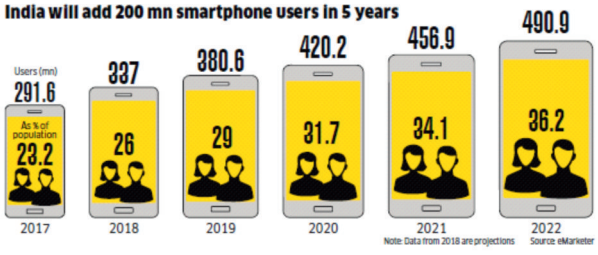
users of smartphones with suboptimal understanding of security protocols, including what is safe to click and what might not be.

No one quite knows how they are using the internet and what apps are being installed on these devices. They are also likely to be less circumspect about sharing data with app developers. Most terms and conditions that users agree to tend to be in English. Fair to assume that many Indian mobile users are agreeing to things without quite understanding what they are agreeing to.

As we settle back into the chairs at his Delhi-based office, Modi says it is relatively harder to install malware on Apple's iPhones. To install a hacking app on an iPhone, you need the unique device identifier — a sequence of 40 letters and numbers, which can only be accessed by connecting the phone to a computer via Apple's iTunes software. "It is far easier to install an app from an unknown source on an Android phone than on an iPhone," says Modi. According to data aggregated by Lucideus, Android (all versions combined) has 1,855 known vulnerabilities, compared with 1,495 for iOS.

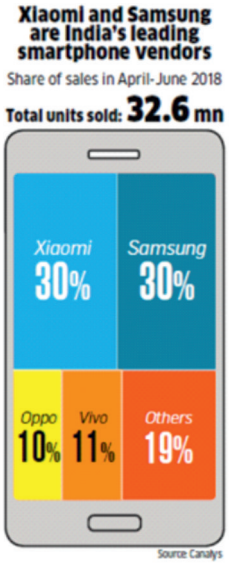
Outdated privacy laws in India add to the woes of mobile phone users, say industry watchers. "In India, the regulations are weak at best," says Shiv Putcha, founder of telecom consultancy Mandala Insights. "You don't have a privacy law, no regulations around data storage or access to private data. If they (mobile phone makers and service providers) aren't storing data here, how can we be sure how secure our data is?"

The user has little chance of bringing culprits to book in case of a data breach, as most companies aren't liable to the user in India. "The business model (of the smartphone) doesn't fit local regulation, because there isn't one. As more cheap devices are sold, this problem doesn't just compound, it explodes," says Putcha.



The Telecom Regulatory Authority of India (Trai) said this week the framework for data protection was "not sufficient" to protect consumers. It also recommended that ownership of data generated by telecom consumers should rest with the users and not internet giants and mobile device makers. The government has woken up to the need for a strong data protection law, along the lines of the General Data

Protection Regulation (GDPR) in the EU, and has set up a committee to look into it.



With smartphones and data becoming cheaper, the number of devices, apps and the time spent on these will increase. The ensuing data explosion gives hackers more opportunities to exploit. Nearly a decade after Android was commercially released in September 2008, the mobile OS developed by Google might be becoming a victim of its own success. The European Union slapped a $5 billion penalty on Google earlier this week for abusing the market dominance of Android to push its search engine, a decision Google will appeal.

The world got a taste of large-scale hacking three years ago, when cyber security firm Zimperium said it had discovered a bug called Stagefright that rode on an innocuous-looking multimedia message to take over Android phones. Over a billion phones were reportedly infected.

Large-scale Risks

Modi says even legitimate apps can get your data by simply asking for access permission. While the Gionee phone used in this demonstration was running an Android 5.1, a three-year-old version of the OS, Modi warns this is possible on recent editions of Android as well, which are supposed to be far more secure. Besides apps, vulnerabilities are also found in the OS itself, chipsets or the cellular or Wi-Fi network.

A fair number of phones in India are still vulnerable despite all the security patches, says Peter Eckersley, chief computer scientist, Electronic Frontier Foundation. "This problem needs to be tackled systematically by telecom companies and handset manufacturers. These people are in a position to send Google's security updates to their users, but usually don't. A bigger concern than individual phones being compromised is that vulnerabilities create large-scale cyber security risks, where a single piece of malware can infect a huge number of devices in a short period of time," adds Eckersley.

For the bulk of the over two billion Android devices in the world, Google provides the base OS and regularly releases updates or security patches. Handset makers such as Samsung, Xiaomi and Huawei make their own modifications to the operating system. The customisation could be tweaks, the addition of apps and features (like what Samsung does) or an overhaul of the OS to give it a different look (Xiaomi's MIUI being a case in point). Many manufacturers also offer their own app stores.

Android's Recent Security Lapses

April 2018: Vendors such as Gionee, Oppo and Lenovo had **missed four or more security patches,** Berlin-based Security Research Labs said after a study of 1,200 Android phones

March 2018: A news report revealed **Facebook got access to Android users' calls and SMS logs through its apps,** thanks primarily to lax permission standards in older versions of Android

November 2017: A report by Quartz said **Google had been collecting location data of Android users even when users had turned off location services**; Google said it would stop the practice

November 2017: Investigation by Yale Privacy Lab and Exodus Privacy revealed more than three-quarters of the **300 Google Play apps tested had hidden location trackers and targeted advertising,** among others

December 2017: Trend Micro Mobile Security found **36 apps on the Play Store that secretly harvested user data and tracked user location;** Google removed these apps later

Google's updates can take time to reach the users because the phone makers make modifications to the updates to factor in their features. Less than 6% of Android phones in India have the previous major OS release, Android Oreo (8.0 or 8.1), says StatCounter. Both Android Oreo 8.0 and iOS 11 were released in August-September 2017. Android P, announced in March 2018, is still in beta stage. Nearly three-quarters of iPhones, on the other hand, are running the last major release, iOS 11, or minor updates to that verson.

Harmful Apps

According to Google, in 2017, India had the third highest percentage of phones with potentially harmful applications (PHAs) among the major Android markets, with 1% of the total Android phones in the country affected, though the figure had dropped by a third from 2016. Google says devices that install apps from outside the Google Play app store are nine times more likely to have PHAs. A Google spokesperson did not respond to India-specific questions but pointed to two measures the company has taken to improve phone security in the country.

One is a partner-certification programme that was launched in August last year. Devices of some 140 vendors come with Google Play Protect feature, with automatic scans for malware. The company encourages phone buyers to look for the Play Protect logo on smartphone boxes ahead of purchase. It also ran a #SecurityCheckKiya public campaign earlier this year. Samsung, one of India's leading smartphone vendors by unit sales in April-June, says it provides monthly security updates to its top and mid-range devices, and quarterly security updates to the rest.

"Security updates by Samsung already include all the security patches of Android provided by Google and also include patches for other vulnerabilities discovered," a company spokesperson. ET Magazine's questions to Xiaomi and Vivo, other major players in the market, remained unanswered. Updates, though useful, are usually not a favourite among users either. They fear these might make phones slower. There are also several who do not even know what an OS update or security patch is, and couldn't care less.

"If you don't have access to safe drinking water or medicines in your village, then mobile malware on your smartphone is hardly your biggest issue," says David Rogers, CEO of UK-based mobile security consultancy Copper Horse. iPhones are widely believed to be more secure because Apple controls both the hardware and the software.

Google's Pixel and, to an extent, the older Nexus devices also fall into this category. Developers say Apple is a lot more stringent in its app-approval process, too. The process involves more human intervention on iOS than on Android, according to Sean O'Brien, lead technologist, Yale Privacy Lab. "There is a wider proliferation of bad apps on Google Play (than App Store)."

Google is trying to bridge the gap on the app front. Last year, it removed 7,00,000 bad apps and 1,00,000 developers from Google Play. Last year also saw a 30% rise in the number of Android devices getting security patches, though it is not known what percentage of Android devices got the latest security patches. A study of 1,200 Android smartphone models by Berlin-based Security Research Labs revealed many companies do not issue security patches, as was being claimed by the phone makers. Handset makers such as Vivo, Oppo and Gionee have missed four or more security patches, according to the results of the study, first reported by Wired in April.

National Security Concerns

Lax permission standards in the older versions of Android were said to be primarily responsible for Facebook getting access to users' call and SMS logs through its apps, according to news reports that came out following the Cambridge Analytica controversy in March. Late last year, Trend Micro Mobile Security found 36 apps on Google Play that secretly harvested user data and tracked user location. Once notified, Google removed these apps.

A month earlier, an investigation by Yale Privacy Lab and Exodus Privacy revealed more than three-quarters of the 300 Android apps that were tested had hidden codes for location tracking and targeted advertising, among others. In May 2017, reports emerged that more than 36 mn Android users worldwide may have downloaded one or more of the 50 apps with a malware called Judy, which made use of the devices for false clicks on online advertisements.

Besides the violation of an individual's data privacy, there is also the matter of national security. Raghu Raman, former CEO of the National Intelligence Grid, who now serves as group president for risk, security and new ventures at Reliance Industries, says the problem goes well beyond the mobile OS that we use. "We tend to forget that the base hardware isn't made by us, nor is much of the software, including the anti-malware tools meant to keep us safe."

He does not think it is a great idea for the government to use the telecom gear we buy from a potentially hostile country, even if it is vetted by a friendly country. "We'll just have two pieces of malware to contend with in that case, rather than one."

Given the cloudy provenance of a lot of the apps we use, combined with the proliferation of Chinese handset makers, the government will have to keep a close eye on the situation. The last thing it needs is the personal details of millions of Indians ending up in the hands of non-state actors or countries that India is not particularly friendly with. The Defence Ministry in December asked security personnel to uninstall over 40 apps from their mobile phones, most of them Chinese, including WeChat, NewsDog and UC Browser. These remain among the most downloaded apps in India.

Raman fears someone can use contact information to geo-locate where an army commanders' meeting is happening or where a group of important politicians are meeting. "I don't even need their so-called confidential numbers. I just need the staff officer or PA's contacts and I can say where they all are."

The PoleStar Foundation
e-mail: polestarfoundation@gmail.com
www.polestar-foundation.org

Follow us: @polestarawards
facebook.com/PoleStarAwards

For further information, contact:
Divya Narayanan - +91 9500168543